WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Countering Rogue Drones: India's Legal and Technological Response to Unauthorized Autonomous Drone Activities

Aman Kumar Thakur[1], Dr. Ratnesh Kumar Srivastava[2]

[1]Student, B.A. LL.B. (Hons.), Law College Dehradun, Uttaranchal University, Dehradun, Uttarakhand, India.
[2]Head of Department and Associate Professor, Law College Dehradun, Uttaranchal University, Dehradun, Uttarakhand, India.

ABSTRACT

India's growing drone industry, supported by government initiatives and rapid advances in technology, now faces an ever-intensifying challenge from unlawful activities perpetrated by autonomous drones. The Drone Rules, 2021 and subsequent amendments in 2023 were an attempt to foster a more progressive environment for regulation of human-operated UAVs; however, a similar environment does not exist for AI-driven autonomous systems. These drones function autonomously, increasingly avoiding detection, crossing into restricted areas, and engaging in activities that may be regarded as illegal, such as smuggling and spying. All technological solutions, such as the D4 system developed by DRDO and vehicle-mounted counter-drone units, face the problems of high costs, scalability, and real-time enforcement. The tort law framework governing the liability issues in question, together with an unclear liability scheme, somehow complicates the regulatory approach to autonomous drones. These issues became evident from events reported from international borders and within some Indian cities, much after the incidents drew public attention. The paper analyses existing gaps in the law and technology, with analogies from Indian case laws and counter-drone technology, to design an approach from multiple angles: AI-specific laws, a stand-alone drone authority, and graduated penalties, all coupled with ethical codes to guide use of countermeasures and public engagement mechanisms. An aligned regulatory oversight mechanism must prioritize technologies in furtherance of national security, public safety, and privacy interests and finally support India's 2030 vision to become a global drone hub.

Keywords: Autonomous drones, Drone Rules 2021, counter-drone technology, airspace security, AI regulation, DRDO D4 system, privacy violations, India UAV policy.

Introduction

AI-enabled autonomous drones are changing industries in India by performing off-the-shelf tasks with rare human intervention. In agriculture, drones operating in tandem with startups such as Garuda Aerospace undertake precision spraying, which diminishes pesticide usage by 30%. In logistics, drones ferry items for last-mile delivery, with companies like Zomato piloting autonomous systems. Infrastructure is monitored by surveillance drones whilst defense watches underscore reconnaissance by DRDO-developed UAVs. Having pegged the value of the Indian drone sector at $1.2 billion in 2024, it is forecasted to grow at 25% annually, underpinned by the federal Production Linked Incentive (PLI) scheme. The mushrooming of the drone market has given rise to fears of unauthorized operations and hence requires tight scrutiny.[1]

Under the effect of artificial intelligence, drones truly change industries in India as they perform with very little intervention of humans. In agriculture, drones such as those of Garuda Aerospace would do precision spraying with up to a 30% reduction in pesticide use. Logistics sees drones assisting last-mile deliveries, with autonomous systems being tested by companies like Zomato. Surveillance drones would watch over infrastructure, whereas defense sees their application as reconnaissance from the DRDO-developed UAVs. The Indian drone market was valued at $1.2 billion in 2024 and is expected to grow at 25% CAGR with incentives under the Production Linked Incentive (PLI) scheme. With this proliferation, however, there is piracy, and therefore strict measures have to be taken in person.[2]

Policy initiative from the Government of India backed this ambition of positioning India as a global drone hub by 2030. In 2022, the Ministry of Civil Aviation came up with the Drone Shakti initiative to foster drone startups and innovation hubs. The Drone Rules 2021 cut down the regulatory burden of compliance, thereby ensuring a suitable environment for the manufacturers. The government utilizes drones for rural land mapping under the SVAMITVA Scheme, presenting a typical example of public-sector application. More than 200 startups are working in the drone ecosystem in India today; they are

[1] Ritika Rathi, Sreetama Sen, et.al., "Hovering over us – Drones in civil use", available at: https://corporate.cyrilamarchandblogs.com/2020/05/hovering-over-us-drones-in-civil-use/ (Visited on April 8, 2025).
[2] Countering Rogue Drones: Challenges and Technologies, available at: https://defence.capital/wp-content/uploads/2019/08/countering-rouge-drones.pdf (Visited on February 23, 2025).

backed by a number of tax benefits and comparatively relaxed foreign investment norms. But the rise in the autonomous use of drones has outpaced the development of the regulatory framework, creating loopholes.

Ever since, unauthorized drones represent serious threats to national security, especially for sensitive installations such as strategic borders and military establishments. Such problems have only been exacerbated by happenings in the western borders of India in 2025, with drones being used to smuggle contraband. Often working through AI to hide themselves in the radar systems, drones are indeed a new challenge to the age-old security setup. The Drone Rules, 2021, govern them, including for prohibition of flying near strategic installations, but much ill will and poor enforcement seem to have crept in.[3]

Unauthorized, illegal autonomous drones can pose threats to national security, especially in sensitive areas such as borders and military installations. The cases of drones smuggling contraband across the western border of India in the year 2025 have acted as warning signals. The drones are AI-empowered to evade detection, thus challenging the usual way of securing. The Drone Rules, 2021, prevent flights near strategic sites, but enforcement is yet to take shape.

Infringing upon individual privacy are rogue drones equipped with cameras, gathering information without consent in both urban and rural settings. The Digital Personal Data Protection Act, 2023, provides some protections, but its applicability to drones remains to be tested. Safety risks emerge when incidents take place where near misses of January 2024 were reported when drones flew close to airports or crowded events. One could rely on this Anuj Garg v. Hotel Association of India (2008) case on public safety regulations as a legal analogy for drone regulations. With no case law addressing the issue, tort liabilities in negligence may apply, but these are not adequate for autonomous systems, necessitating comprehensive regulatory frameworks.

Legal Framework Governing Drones in India

When the Civil Aviation Ministry first brought it to notice on 25th August 2021, the Drone Rules, 2021, was legislation to design an all-inclusive mechanism to govern the Unmanned Aerial Vehicles (UAVs) in India. Contrasting with the highly complicated Unmanned Aircraft System Rules, 2020, these rules were meant to encourage innovation while having regard for safety and security concerns. Aiming to simplify, the Indian government indicated its desire to be branded as a global drone hub by 2030, propagating the use of this technology in agriculture, logistics, and surveillance. With the increasing use of drones, these rules attempted to curb unauthorized drones, and the challenges remain with autonomous drones that possibly require hardly any human intervention and therefore need regulatory amendments.

The Drone Rules, 2021, had removed many bureaucratic hurdles by scaling down the permitted number of forms from 25 to 5 and eliminating any security clearances for drones used for non-commercial purposes. In this way, the simplified rules would encourage startups and small operators into participation to help bolster the sector. There was rationalization of fees into four bands-the cheapest-and permission was no longer required to fly drones in green zones. This fits into India's vision for a friendly drone ecosystem. The simplified processes, meanwhile, are relevant only for human-operated drones; the perspective of autonomous drones needs to be taken care of through very different compliance mechanisms, given their AI-driven robotic operations.

Key Regulatory Provisions

The Digital Sky Platform is one of the pillars of the Drone Rules, 2021, which provide a digital interface to control drone operations in real time. Operators use it to register drones, apply for pilot certificates, and receive flight permissions. The platform prohibits drone operations in areas designated as red zones; flight activities in yellow zones require prior approval; and those in green zones are permitted subject to notification. The platform's real-time tracking capability allows authorities to see any breaches, which is of paramount importance in detecting illegal drone activities. It will be able to work efficiently against usual drones, but in the case of autonomous drones, which may even evade tracking by standard means due to their higher AI capacity, the platform curtails such monitoring capacity-a grave concern that calls for certain technological interventions so as to ensure strong enforcement.[4]

Remote Pilot Certification Standards

The fourth rule under the Drone Rules, 2021 sets forth that all drones, provided they do not fall in the Nano category under which drones weigh less than 250 grams, shall be registered with a Unique Identification Number-UIN. The UIN aids in tracing drones to their respective owners to hold them accountable for any wrongful or illegal operations that may ensue. All registration must be done through the Digital Sky Platform, which maintains a centralized database. Any breach of this will invite penalties to compel observance. This, however, proves easier said than done when an autonomous drone might fly independently and real-time violation mapping with a UIN appears difficult if not impossible, as its AI systems may obfuscate and shield the operator's identity. This begs the profile of advanced identification technology to aid in the enforcement of regulations.

Restrictions on No-Fly Zones and Activities

Remote Pilot Certificate must be obtained from DOJ-accredited training organizations by operators of drones weighing over 2 kilograms or being used for commercial applications. The training covers airspace rules, safety regulations, and flying skills, thereby instructing responsible use of these drones.

[3] Countering Rogue Drones: Key Anti-Drone Jamming Techniques, available at: https://flymoredrone.in/blog-details/countering-rogue-drones-key-anti-drone-jamming-techniques (Visited on February 24, 2025).

[4] My New India Story Podcast Episode 1: Countering Rogue Drones, available at: https://www.investindia.gov.in/team-india-blogs/my-new-india-story-podcast-episode-1-countering-rogue-drones (Visited on February 26, 2025).

Certificates are a must to prevent misuse overpowering safe areas. But an autonomous drone operating under AI means that the requirement is irrelevant as its operations will not pass through any pilot's oversight. Accordingly, this difference calls for new certification mechanisms for AI-driven systems, bringing in accountability for autonomous drone activities in the Indian airspace.[5]

Penalties for Unauthorized Drone Operations

India has a regulatory framework with the Drone Rules, 2021, issued to lay down a series of penalties for discouraging illegal drone activities. These include fine imposition and administrative actions, and in very serious cases, criminal prosecution. The accountability is to be created so that drones are not misused in areas where they are strictly prohibited or sensitive. While these penalties prove effective against human-piloted drones, it has limitations when applied to a fully autonomous system.

Enforcement should also evolve quicker with drone technology, with penalties depending on the level of threat posed by each kind of unlawful drone activity. Close these gaps, and airspace control can be preserved over India, which is already congested.

Financial and Administrative Sanctions

Enforcement mechanisms will have to keep pace with the rapid evolution of drone technology, with penalties varying as per the degree of threat posed by a given kind of unauthorized drone operation. If these loophole-escape situations are plugged, India, already choking with congestion, shall retain its control of airspace.

Criminal Liability Provisions

Drone Rules, 2021, under the Indian governance framework, provides for various penalties to deter illegal drone operations. Depending upon the gravity of the act, penalties can consist of monetary fines and administrative actions, while at the highest end in grave situations, criminal prosecutions are undertaken. In order to prevent drone operations in restricted or sensitive areas considered unsafe, it is necessary that these penal provisions be used to hold a person accountable for any kind of action. These penalties would otherwise suffice if drones were human-operated but have proved insufficient against autonomous systems. As the whole field of drone technology shifts rapidly, enforcement must keep pace just as rapidly, with penalties taking into account the differing degree of threat posed by each kind of prohibited activity. The filling of these loopholes is a necessity to keep on with surveillance activities in the ever-congested airspace of India.[6]

Enforcement Limitations

Grievous offenses that put public safety in peril may result in crimes under the Penal Laws, particularly those under Section 336 of the Indian Penal Code, dealing with acts done with so reckless disregard for human life that they endanger human safety. An offense threatening the security of the nation would invoke the Unlawful Activities (Prevention) Act, 1967, and stringent consequences would be assured. In the absence of specific criminal laws against drones, prosecution becomes tricky, making it particularly hard in the case of autonomous drones: intent of the operator in AI-driven operations becomes all but impossible to prove. To this end, the legislature must create penal provisions that specifically deal with drone-related offenses so that clear legal responsibility attaches to those drone activities that lead to unlawful consequences and authorities can begin to confront the special problems posed by unauthorized autonomous drone activities.

Updates Via Drone (Amendment) Rules, 2023

The enforcement of penalties under the Drone Rules, 2021, has been difficult due to lack of real-time detection and minimal coordination among the Directorate General of Civil Aviation, the Central Government, and local police. The Digital Sky Platform attempts to monitor, but covering the entire nation, especially the remote regions, remains challenging for it. With autonomous drones, the matter is even graver as with an inbuilt decision-making AI, they can simply counter any conventional surveillance method. Strengthened enforcement should promote integrated operation of counter-drone technologies such as radar, jammer, and the platform and forming backup task forces. In short, better inter-agency collaboration backed by investments in relevant technologies will create an environment where the threat of enforcement will actually deter unauthorized drone operations in India.

The Drone (Amendment) Rules, 2023, notified ben on 27th September 2023, amended those of 2021 with the aim of making them more user-friendly and easy to comply with. Responding to the stakeholders' comments, amendments were introduced to foster the interest of small operators, many of whom operate in rural areas, thus also aligning with the inclusive economic policies of India. By removing these regulatory hurdles, the rules promote the lawful adoption of the drone, especially in areas where they do not give priority. These amendments show India's will to develop a lively drone ecosystem while keeping in check the possible misuse thereof. Nevertheless, the emphasis on human-operated drones narrows down its scope to an application of autonomous drones, thereby clearly suggesting further amendments in the domain of AI to take care of such regulatory issues.[7]

---

[5] National Anti-Drone Guidelines, available at: https://www.drishtiias.com/daily-news-analysis/national-anti-drone-guidelines (Visited on February 27, 2025).

[6] What Technique Best Defeats Rogue Drones?, available at: https://www.unmannedairspace.info/commentary/what-technique-best-defeats-rogue-drones/ (Visited on February 28, 2025).

[7] A Brief on Counter-Drone Technologies: Countering Rogue Drones, available at: https://www.linkedin.com/pulse/amr-future-brief-counter-drone-

The 2023 amendments facilitated Remote Pilot Certificate requirements by allowing government-issued IDs like Aadhaar to be used in place of passports while reducing documentation. This ease in certification opened up possibilities for rural operators and small-scale drone operators. Abiding by set safety regulations requires an increased number of certified pilots, which is the object of the process. These modifications reduce barriers to drone use for agriculture and logistics applications. However, for autonomous drones, which have no relevance to human pilots, the certification framework fails, establishing a need for AI-driven operations regulations to account for governance so applications are not directed parallelly.[8]

Technological Measures to Counter Rogue Drones

Amendments in 2023 augur well for the rural and small-scale sectors, which utilize drones for crop monitoring and land surveying under schemes like SVAMITVA. Easy certification allows farmers and small businesses to take advantage of drone technology to increase their revenues and support economic inclusion. The emphasis on accessibility promotes sustainable utilization of drones in the framework of India's rural development. Autonomous drones, increasingly utilized in rural setups for automated operations, are not discussed in these amendments. Including AI-driven systems within the regulatory scope is essential to prevent illegal operations and secure airspace in the rural areas.

The counter-drone technologies have been developed to detect, disrupt, and neutralize unauthorized drones, with the principal technologies falling into three main categories. Detection technologies use radars and radio frequency sensors to detect drones either by their signals or by their very existence. Disruption technologies include jammers, blocking communication between drones and their operators or GPS signals to force drones to either land or return home. Neutralization technologies target drones physically and might include lasers and more kinetic systems. These systems come to the rescue in case of rogue drones posing threats in either civilian or military arenas. The existence showcases attempts worldwide to counter the rising threat of autonomous drones, especially those with high levels of AI capabilities.

On a global scale, counter-drone technology has swiftly developed in response to the spread of drone technology. Consider for example how the United States and Israel have deployed many complex systems. One of these is the DroneSentry-X, which integrates radar and jammers to allow for real-time responses. The emphasis in Europe is on regulatory integration, with solutions such as SkyWall that utilize a net to capture. The advancements have been made to pinpoint threats to minimize collateral damage, something that becomes quite relevant with urban settings. Other upgrades have brought in AI-powered analytics which allow for faster threat identification and modularity for system scaling-up or down. Such global developments inform India's approach wherein the challenge remains in modifying these technologies for densely populated urban landscapes and sensitive border areas, thereby ensuring the effective mitigation of rogue drones.[9]

India's Counter-Drone Innovations

Drdo's D4 System

India's densely populated urban centers, such as Delhi and Mumbai, and its sensitive border area, mainly along the Line of Control, require special counter-drone systems. Rogue drones threaten public safety in the cities, disrupting air traffic or conducting illicit surveillance, while bordering acts of encroachment demand security of the nation. The said technology has to be challenged by high levels of electromagnetic interference in urban areas and also be adapted to rugged landscapes along borders. India's diverse geography and population density can ideally demand scalable and cost-effective solutions that can integrate with existing airspace management systems. These constitute challenges that if tackled will become safeguards to India's infrastructure and security, thus making counter-drone systems a matter of utmost concern to India's advancement and civilian welfare.[10]

Vehicle-mounted Counter-Drone System

Drone Detect, Deter, Destroy (D4) System is a flagship project focusing on urban security, being developed by the DRDO. The D4 acts in defense against rogue drones, deploying three key layers: radar, RF sensors, and laser technology, installed in high-risk areas. It provides a multi-layered protection for every stage of a threat that includes detection and action against it. The system was built for fast actions to neutralize drone attacks in highly dense cities, guarding critical infrastructure such as Government buildings against attacks from rogue drones. This development of the D4 system points towards the Indian view for indigenous development, thereby reducing license dependence and creating self-reliance in antidote drone capabilities; this becomes necessary to deal with an autonomous drone threat effectively.[11]

Collaboration with Bharat Electronics Limited

Aero India 2025 saw the inauguration of the mobile counter-drone system vehicle, which fortifies India's mobile defense capabilities in a joint development between Adani Defence and DRDO. This counter-drone system mounted on tactical vehicles combines radar, electro-optical sensors, and

technologies-countering-zkmhc/ (Visited on March 1, 2025).

[8] News Desk, "Indian Ministry of Civil Aviation issues order to ADSTL to set up counter drone system", *Geospatial World*, March 30, 2021.

[9] 10 Counter-Drone Technologies to Detect and Stop Drones Today, available at: https://www.robinradar.com/resources/10-counter-drone-technologies-to-detect-and-stop-drones-today (Visited on March 2, 2025).

[10] Press Trust of India, "Need To Invest More In Research To Counter Rogue Drones: Industry Body", *NDTV*, June 28, 2021.

[11] National Counter Rogue Drone Guidelines, available at: https://sflc.in/policies-and-cases/national-counter-rogue-drone-guidelines/ (Visited on March 3, 2025).

jammers for detecting and disrupting drones on the move. It is an exciting feature indeed, aiding the security of short-term events like public gatherings and patrolling border areas. The modular structure permits upgrades, allowing it to remain relevant to changes in drone technology. This development advances India's ability to counter rogue drones in a dynamic environment, providing adaptable and field-operable technology for the safety of civilians and military.[12]

Operational Mechanisms

Partnerships with Bharat Electronics Limited (BEL) are hence critical in scaling India's counter-drone technologies. The option to avail BEL's domain expertise in defense electronics ensures mass production of items such as D4 and vehicle-mounted systems with cost efficiency and reliability. The partnership basically utilizes the manufacturing infrastructure of BEL to satisfy the national demand and allow for deployment in urban and border areas. Such collaboration enhances the ambiance of public-private partnership in India, intertwining its technological growth with the idea of Atmanirbhar Bharat. Integration of counter-drone systems with national command networks lies with BEL, which will further work on bettering coordination among different defense and civilian agencies to implement measures to counter unauthorized autonomous drones in varied operational environments.

Detection Capabilities

Several methods exist for counter-drone operations, one of which is a layered approach consisting of detection, disruption, or neutralization. With every stage, a threat posed by unauthorized or rogue drones is detected and handled. These systems have to act together to unleash a timely and adequate response, especially while protecting sensitive areas such as borders, airports, and urban centers.

The Indian anti-drone operation integrates technologies over these principles to ensure airspace security. Also, understanding the technical basis of every element of operation aids in recognizing their strengths and weaknesses, thus better coordination, accuracy, and enhancement with changes of drone threats.[13]

Disruption Techniques

These technologies are integrated in the Indian air-defence operation to maintain airspace security. Understanding the technical underpinnings of each operational component helps in understanding their strengths and limitations and hence in their better coordination, use, and improvement in line with changing drone threats.

Now, even more advanced RF sensors locate drones by analyzing the signals emanating from drone communication. These systems prove vital to tracking down small drones or autonomous drones that might manage to evade conventional surveillance. The Indian government deploys these technologies in urban centers and border areas for preemptive warning against rogue drones. Continual upgrading of these systems would counter AI-driven drones with stealth, thereby furthering detection accuracy in some complex environments.

Neutralization Methods

Disruption technologies, primarily jammers, disrupt drone communications by emitting signals that block control frequencies, resulting in forced landings or returns. Modern jammers are designed to interfere with selected bandwidths only, so as not to prevent legitimate communications from taking place; thus, they may be used in urban areas. In India, these systems find their applications mounted on D4 and vehicle platforms to serve in non-lethal means of interdiction. Their ability to function effectively rests on real-time data provided by the detection systems and thereby allows pinpoint targeting. Yet, jamming may be ineffective against autonomous drones that follow pre-programmed flight paths and, therefore, adaptive means must be developed to retain control over India's airspace and counter these acts of subversion.[14]

Limitations of Current Technologies

Neutralization involves cancelling rogue UAVs by way of high laser or kinetic means. Lasers in systems such as D4 engage targets up to a maximum of 3 kilometers on critical points. Kinetic systems deploy nets to collect drones for forensic analysis. These methods are suitable in a very high-security zone but are not so efficient when used in a populated setup because of the higher possibilities of collateral damage. India has put its focus on laser technologies, meaning it is striving in the areas of cutting-edge solutions. However, the application of these technologies in an urban setup still needs well-laid protocols. Neutralization ensures thereby a decisive act towards a persisting threat, in particular, autonomous drones that manage to evade detection or disruption.[15]

Detection Challenges in Urban Environments

---

[12] Adani Defence and Aerospace at Aero India 2025, Adani Enterprises (February 2025), available at: https://www.adanienterprises.com/en/newsroom/media-releases/adani-defence-and-aerospace-and-drdo-unveil-india-s-vehicle-mounted-counter-drone-system (Visited on March 18, 2025).

[13] Counter-Drone Technologies: The Legal Challenges, available at: https://www.nishithdesai.com/SectionCategory/33/Technology-Law-Analysis/12/60/TechnologyLawAnalysis/4409/3.html (Visited on March 4, 2025).

[14] Countering Rogue Drones, available at: https://chintan.indiafoundation.in/articles/countering-rogue-drones/ (Visited on March 5, 2025).

[15] Nadeem Inamdar, "AFS installs drone system to counter threats from rogue UAVs", *Hindustan Times*, December 10, 2023.

Counter-drone infrastructure possesses certain limitations that make it difficult for authorities to respond speedily and accurately, with sufficient coverage, against rogue drone threats. Detection, disruption, and neutralization methods are evolving; however, real-world situations pose challenges to present systems-especially in urban or very congested areas. These limitations include limited detection accuracy, chances of interference with signals, and prohibitive costs of deployment. Such challenges hamper the effectiveness of any counter-drone solution, which already has to deal with situations in which swift and accurate implementation is required. In order for these limitations to be worked around, investments must be made in intelligent technologies, adaptive protocols, and cost-effective and scalable solutions that are suitable for India's varied geographic and demographic settings.

Risks of Signal Interference

Small or low-flying drones are very hard to detect in cities, owing to physical obstructions such as buildings and electromagnetic interference stemming from communication networks. Small drones weighing less than 250 grams are practically invisible to the radar. An autonomous AI-powered drone poses an additional challenge for detection, causing the unusual alteration of flight patterns. These constraints hinder the timely identification of threats in India's densely populated cities, hence increasing risks to public safety. It is thus imperative to develop AI-based detection systems and multi-sensor fusion technologies to increase the precision with which rogue drones are picked up in complex urban settings.

Cost and Scalability Issues

Signal interference poses a major limitation to counter-drone systems deployed in urban areas. Jammers are rogue-drones' nightmare in their operations and can interrupt legitimate communications such as for Wi-Fi or for emergency services, which is an unintended consequence. Where digital connectivity is serious business in urban India, the whole deployment problem gets seriously complicated. And there would be the weather or some pollution to lessen the already existing reliability of the electro-optical sensors. The solution may be jammers targeted to specific frequencies and the development of adaptive algorithms for reducing collateral damages from jamming. In this respect, India must then spend enough resources on technology that balances the needs of counter-drone activities with respect to uninterrupted communication networks for civilian life in metros.[16]

Regulatory and Technological Challenges

Counter-drone systems, including radar, lasers, and jammers, cost too much to be deployed all over India. Systems like D4 and vehicle-mounted units require vast chunks from installation to land infrastructure, giving rise to challenges to be considered in making the countermeasures widespread. Scalability also suffers since trained operators have to be found, having to be melded into the workings of the existing airspace management. Given the amalgam of urban and rural profiles into an Indian landscape, it calls for cost-effective solutions. Pragmatic means can be set up through public-private partnerships such as with BEL and modular types of systems to allow for a full-scale counter-drone deployment across India to curb effectively rogue drone threats.

Gaps in the Legal Framework

The very rapid adoption of drone technologies has outpaced the currently available legal and technical framework on the subject in India, generating various regulatory and operational challenges. Drones have applications in delivery, surveillance, agriculture, and disaster response. But left unchecked, drones can pose serious dangers. Rogue operations, particularly those run by autonomous systems, emphasize the urgency of bringing in new sets of laws and enforcement mechanisms. Without regulation, technological frameworks, and the coordination of these, India's capability to monitor the safe and lawful use of drones is visibly limited. Hence, these aspects need to be addressed to shelter the airspace, face up to public safety concerns, and guarantee data privacy, all while granting drones the space to innovate responsibly.

Lack of Regulations for Autonomous Drones

The Drone Rules, 2021, and other regulations in place in India are simply not enough to deal with the emerging threats posed by autonomous and AI-enabled drones. The rules, while applicable for systems that are manually operated, are simply not an adequate response for drones that operate independently. The lack of detailed provisions for autonomy, enforcement, and accountability becomes a serious loophole. With the development of drone technologies, there is, therefore, vast exposure for parties using or to be confronted by the authorities, such as in terms of operational violations or insoluble liability issues. It is imperative to maintain the legal architecture well so as to ensure safe, secure, and responsible drone usage in this dynamic airspace environment over India.[17]

Inadequate Real-Time Enforcement

Having no mention of fully autonomous drones created by AI and working with no human intervention in the Drone Rules of 2021 means they are created relatively unnamed, thereby giving them some slight loopholes since AI drones will not comply with mechanisms meant for human-piloted systems, such as the option of self-navigation. The absence of a proper provision undermines the enforcement. The enforcement is even more difficult when rogue drones wreak havoc. The rules dictate thrice registration, and pilot certification does not come into play for autonomous systems; therefore, authorities

[16] Drone Threat is Real: India Needs a Comprehensive Counter-Drone Strategy, available at: https://www.vifindia.org/article/2023/june/09/Drone-Threat-is-Real-India-Needs-a-Comprehensive-Counter-Drone-Strategy (Visited on March 18, 2025).

[17] Countering Rogue Drones Menace in Absence of Real System, available at: https://bharatshakti.in/countering-rogue-drones-menace-in-absence-of-real-system/ (Visited on April 2, 2025).

have no way to truly deal with their risks. Such targeted regulations have to be developed for AI-empowered drones so that they are held accountable and to keep India's airspace free from misuse.

Uncertainty in Liability Allocation

Without instant detection and penalizing mechanisms, India finds itself limited in real-time drone regulation enforcement. While it can monitor ones that are registered on the Digital Sky Platform, it cannot track illicit or autonomous drones operating outside its network. Ground surveillance and police are too slow to respond in huge metropolitan areas or border points. Rogue drones can take advantage of this and escape penalizing processes under Rule 10 of the Drone Rules, 2021, thereby reducing deterrence. Enforcement must be strengthened with integrated detection systems with dedicated response units so that it acts swiftly on infringements and remains a credible threat to autonomous drone threats.

Technological Barriers

The Drone Rules, 2021, have ambiguities on responsibility for damages inflicted by rogue drones. Particular emphasis on autonomous drones needs to be clarified. It is difficult, even impossible sometimes, to put the finger on one point of responsibility when an operation is controlled by AI. For instance, if an autonomous drone engages in collisions or rights violations, who is held responsible-the operator, if at all, since there is little supervision by humans? The absence of clear-cut laws on liability or redress discourages victims from exercising their rights and weakens regulatory enforcement. Establishing a system of liability with defined roles and responsibilities for incidents with autonomous drones will ensure fair compensation for injuries and deter incidents of abuse, thereby aligning Indian laws on drones with challenges that advanced drone technologies pose.[18]

Challenges in Drone Differentiation

Detection is the very first line of defense for any type of counter-drone system that allows radars and electro-optical sensors to identify drones anywhere up to 10 kilometers away. While radars detect the drone movement, the electro-optical sensors are meant to facilitate visual checking of the drones even in adverse visibility conditions.

Lack of System Integration

Increasing drone activity challenges control over Indian airspace and exposes several technological shortfalls that still remain unsettled. While the use of drones continues to proliferate in areas like logistics and agriculture, scant advancements are being made in monitoring systems to distinguish and counter rogue drones. They include weak integration, delayed detection, and enforcement delay due to over-reliance on imported technologies. These technical barriers result in a gap in response, risking the allowing and application of drone-use within India with no attempts that may otherwise afford timely interference. Knowing exactly which technological roadblocks stand in the way of such proceedings will force the creation of a swift and scalable solution that can place a balance on this technology in the interest of the nation's security and the safety of the people.[19]

Reliance on Imported Components

Counter-drone systems of India like the DRDO D4 function on their own devoid of national airspace management-which affects their competence.

Without further integration into systems of the Directorate General of Civil Aviation or the Digital Sky Platform, coordination in real time between detection and disruption, and air traffic control is affected. Such a lag, among others, slows response times when it comes to rogue drones in sensitive environs such as airports. Integrated seamless counter-drone systems would immediately raise alerts while coordinating counterforces with the offender. Interoperability must be made a priority in India, leveraging data-sharing protocols to align counter-drone technologies with the present aviation infrastructure for thorough airspace security against extralegal autonomous drones.[20]

Privacy and Ethical Concerns

Counter-drone technologies in India, which include radar and laser systems, are highly dependent on components that are mostly imported, hence posing scalability as well as self-reliance issues. Critical items such as very high precision sensors and microchips are purchased from various parts of the world, thereby adding to the cost of these systems and also making supply chain disruptions undesirable possibilities. This inhibits the Atmanirbhar Bharat movement, which focuses on indigenous manufacturing. Perhaps an inexpensive and locally manufactured system should be deployed at the national level, especially across rural and border areas. Investment in domestic R&D and collaborative ventures with companies like Bharat Electronics Limited would reduce the need for imports, giving India the capability to produce resilient and inexpensive counter-drone systems tailored to its peculiar security needs.

Privacy Risks from Drone Surveillance

[18] Drone Laws in India, available at: https://legalventureslawoffices.com/2024/01/31/drone-laws-in-india/ (Visited on March 11, 2025).

[19] India's Border Security Challenge: Rogue Drones and Smuggling Surge, available at: https://borderman.in/articles/indias-border-security-challenge-rogue-drones-and-smuggling-surge/ (Visited on March 27, 2025).

[20] Gireesh Chandra Prasad, "Strategy to counter rogue drones in the offing, says govt official", *Mint*, August 1, 2019.

The rapid surge in drone use has brought complex and urgent concerns in the fields of privacy and ethics. While drones offer an array of possibilities in terms of logistics, surveillance, and Research, they also pose dangers to civil rights and public safety if misused. In the densely populated cities of India, the illegal surveillance and careless deployment of counter-drone systems also evoke questions of legality and ethics. Responsible drone operations will hence have to include well-defined boundaries, the strict enforcement of laws, and robust ethical standards applied to all instances of drone and anti-drone technologies.[21]

Misuse of Counter-Drone Technologies

The counter-drone systems in India, such as the DRDO D4, are independent mechanisms that work outside of the realm of national airspace management, thus limiting their effectiveness.

Ethical Issues with Destructive Measures

Unauthorized drones threaten privacy by capturing images or videos without consent. The Digital Personal Data Protection Act 2023 deems data collection lawful only if the said person gives consent, but rogue drones face identity challenges, thus rendering enforcement difficult. Instances of unlawful drone use in cities in India for purposes of surveillance or delivery would be instances violating personal rights by means of unauthorized data capture. It is the unattended live tracking of these menaces that has let the rogue drones dominate the field with impunity. Strengthening the implementation of the DPDP Act on drones, in combination with the installation of counter-drone systems that can intercept violations, would be the best reward for privacy as against legitimate drone use.

Notable Incidents of Rogue Drone Activities

Counter-drone technologies may either jam or use lasers against legitimate drone operators, thus disrupting activities such as agricultural spraying or logistics which have a legal recognition. Any misidentification or aggressive use of counter-drone measures in some urban areas may interfere with the operations of duly registered drones, resulting in economic loss or safety risks. Lack of proper protocols on such operations escalates the risk, wherein the authorities tend to favor security over exactitude. India must have standardized guidelines for employing counter-drone measures so that any in the likes of D4 attacks only unauthorized drones. To build awareness among the public, a clear reporting mechanism must also be established to minimize the chances of misuse and uphold the public confidence in these counter-drone mechanisms that in turn support legitimate drone ecosystems.

Security-related Incidents

With the increasing use of UAVs, especially with small commercial drones, there has been a rise in unauthorized or malicious use. Rogue drone operations range from smuggling and spying on critical infrastructure attacks. Most of these cases largely occurred in conflict zones, near international borders, and around sensitive civilian areas. Yet these rogue drones remain undetectable by established radar systems due to their small size and operation at low altitudes. Their increasing affordability and availability have caused significant security concerns along with regulatory ones. Documenting such cases aids in identifying patterns emerging and fosters the establishment of stronger policy frameworks to prevent the misuse of drone technology in the future.[22]

Cross-border Drone Incursions

Drones have become a significant security threat, thereby underpinning several instances of disruptive potential. Security-related drone incursions have included the unlawful use of drones in proximity to defense establishments, airports, borders, and strategic installations. These operations are inimical to national security, public safety, and critical infrastructure. Most of these incidents exploit regulatory loopholes or the inability of enforcement agencies. In documenting these incidents, policymakers and enforcement agencies will grow in understanding of the methods and tactics envisaged by offenders. In the wake of the evolution of these threats, there must be an emergent response system coupled with an effective mechanism of drone detection to guarantee the safety of the nation and the civilian population.

Smuggling Via Drones

The use of destructive counter-drone means, such as high-energy lasers, in civil or residential zones presents a professional and ethical problem. There lies a faint but possible chance of collateral damage occurring during the destruction of rogue drones-the debris might fall on an unsuspecting person or bear on some kind of property. Autonomous drones which exhibit random, unpredictable behaviors tend to further exacerbate these concerns, since inexact neutralization remains a painstaking process. Damage must be kept to a minimum in countering the threat, least of all in crowded Indian cities. Whenever feasible, a net-based capture system should be employed as a non-lethal method-the lasers could be kept for use in high-security areas. Codifying the ethics of counter-drone operations in view of public safety would very much assist in bringing about a win-win situation for security and humanitarian interests.

National Security and Counter-Terrorism Implications

Multiple cross-border drone incursions have happened in Punjab and Jammu and Kashmir since May 2025, raising extraordinary national security issues. Unauthorised drones, mostly autonomous, were sighted near sensitive military establishments exploiting India's porous boundaries. They were advanced systems of navigation, said to have escaped ordinary surveillance; there lies an obvious hint toward the weaknesses of presently used defense means.

---

[21] Pranav Mukul, "Anti-drone tech rules finalised; deployment based on sensitivity of installations", *The Indian Express*, October 23, 2019.

[22] Strengthening Military Intelligence: The Role of Counter-Drone Systems, available at: https://indrajaal.in/insights/strengthening-military-intelligence-the-role-of-counter-drone-systems/ (Visited on March 14, 2025).

Such infractions incidences should be conveyed to the Border Security Force, bolstering its call for stringent counter-drone arrangements. Such incursion attacks strategic assets whose disruption spells havoc on regional security and thus necessitate further detection technologies alongside landside regulations of the aerial space against such rogue drones that thwart India's integrity from her borders.[23]

Privacy and Public Safety Concerns

Lately, rogue drones have seen a heightened impetus with contraband getting in drugs-and-weapons sort of stuff across the frontiers of India, Punjab particularly. Flying typically autonomously, these drones dropped their parcels under the guise of darkness to avoid any surveillance. The year 2024 saw the interception by authorities of several of such drones laden with contraband, thereby exposing very highly-structured smuggling networks. It is next to impossible for interception to take place when the AI-driven drones themselves are capable of changing their routes to avoid detection. These activities work against law enforcement, so adequate counter-drone systems and international cooperation must be established to effectively cripple cross-border smuggling operations.

Privacy Violations by Unauthorized Drones

The increase in unauthorized drones fitted with the high-resolution option has unleashed and induced high privacy concerns over the urban pockets of India. Illegal drones capture images and videos of private homes and public spaces in close violation of individual rights, with none asked for any permission.

Reports of incidents with drones hovering over private properties in cities like Bengaluru and Delhi have set the alarm among people. Enforcement of data misuse under the Digital Personal Data Protection Act, 2023, may tackle offenses committed by drones whose identities have been ascertained, but in the case of unidentified drones, it would be even more problematic! This very fast-growing concern calls for superior-grade tracking systems that can actually help trace and intercept rogue drones for ensuring privacy in congested urban enzymes.[24]

Near-miss Incidents with Aircraft

Unlawful drones equipped with high-resolution cameras have created a veneer of privacy issues in the urban areas of India. These rogue drones, mostly autonomous, violate consent and death rights by photographing or video recording private residences and public spaces. Such incidents in Bengaluru and Delhi have set the alarm bells ringing, with residents reporting drones hovering over their private houses. The Digital Personal Data Protection Act, 2023, provides for regulating data misuse; however, enforcement against unidentified drones can be near impossible. This burgeoning menace thus deserves to be tracked and countered through the infringement of these drones. This protection of privacy is extremely important in a heavily populated urban setting.

Public Apprehension in Urban Areas

The rogue drones near airports have caused a few near-miss incidents with manned aircraft, thus posing significant risks to public safety. Some of such reports of drones entering restricted airspace near big airports such as those in Mumbai and Hyderabad narrowly missed collisions in 2024. Autonomous drones follow a programmed flight plan that disregards no-fly-zone restrictions. This threatens flight operations and the lives of passengers, pointing to the loopholes in airspace monitoring. Thus, the Directorate General of Civil Aviation (DGCA) has called for its strict enforcement, but owing to the lack of real-time detection, no action can be taken. Activating counter-drone systems at airports must be on priority to disallow such life-threatening risks.

Lessons from Incidents

Giving superhighway to the operators of unauthorized drones with the high-resolution camera option has generated numerous issues over the urban pockets in India. Such unwanted drone operators capture images or video footage of private residences or public spaces; thus, they infringe upon the fundamental individual rights of these persons.

Need for Enhanced Surveillance

Frequent drone-related incidents occurring all over India have exposed great-law lacunas, surveillance capabilities, and public awareness. A drone incident, in effect, brings to light a new vulnerability, which dictates response from various layers. Thus, in a manner of speaking, drone incidents mark down systemic weaknesses that need immediate course correction. The learnings from such incidents should ideally go toward developing smarter policies, better technology in implementation, and citizen participation to protect national interests and public interests.[25]

Importance of Public Reporting Channels

Rogue drone crimes have raised the need for enhanced surveillance of India's airspace. Currently, technologies like the Digital Sky Platform are unable to track autonomous drones that function outside registered networks. These incidents in Punjab and urban spaces bring to the fore lapses in real-time

[23] BL Ahmedabad Bureau, "Adani Defence & DRDO unveil vehicle mounted system to counter rogue drones", *The Hindu Business Line*, February 11, 2025.

[24] K. Bharanitharan, G. Kaur, et.al., "Drones and Surveillance Challenges and Legal Regulation Against Drone Crimes in India", 1 *ICAMAC* 104 (2024).

[25] Sumit Kumar Singh, "Drones to have registration numbers, Air Traffic Police to counter threats from rogue UAVs", *India Today*, January 25, 2023.

detection capable of allowing rogue drones to bypass authorities. Installing advanced radar and RF sensors coupled with AI analytics will provide enhanced capabilities for surveilling airspace and speedy identification of unauthorized drones. Strengthening the surveillance infrastructure, especially the high-risk areas, is, therefore, necessary to prevent security breaches and allow a quick response to any rogue drone activity, be it in plains, mountains, or anywhere else.

Urgency for Legal Updates

To address rogue drone activities, citizens have to be aware about these illegal drone activities and also the media have to provide proper reporting channels, as is the case with urban privacy violation drills. Usually, citizens spot unauthorized drones before the authorities, but the absence of or difficult means of reporting hinders timely actions. If dedicated hotlines or applications for any sightings of drones could be established, it would empower civilians to aid in surveillance. Awareness campaigns focusing on the rules and risks associated with drones will also help encourage public vigilance. In creating a collaborative system between citizens and law enforcement, India could build an active network for rogue drone detection, thereby giving the counter-drone measures a greater impact in both the urban and rural areas.[26]

Conclusion

Repeatedly reported drone incidents in India have shown the gaps in regulation, policing, and awareness amongst the public at large. With every case exposing new vulnerabilities set in layers, an emphasis must be laid on building a multilayered response. These incidences are warning signs of systemic loopholes requiring immediate remediation. Using the incidents as case studies, authorities can draw up better policy provisions, better apply technology, and engage citizens in defense of national and public interests.

The exponential development of the Indian drone ecosystem, a clear indicator for the dawn of the technological renaissance, witnessed proactive governmental policy, entrepreneurial innovation in full glory. Unlike in other parts of the world, where this growth was sluggish and allowed laws and enforcement mechanisms to develop adequately in order to properly deal with the menace of rogue autonomous drones, this was not so in India. The Drone Rules, 2021, along with their 2023 amendments, attempted at establishing the basic regulatory framework. But these laws are focused on manual drones, leaving a large quantum of autonomous AI-enabled drone operations independent. Rogue drones may obstruct national security; infringe upon privacy; jeopardize public safety in sensitive areas like international borders or urban airspace. This, coupled with the incapacity of rogue drones being detected timely and engaging enforcement agencies in coordination, also limits India's capability to counter the said threats, besides poor technological infrastructure. This case law, referenced in the analysis, brings out why the current tort-based liability framework, when applied to autonomous drones, falls short and needs specific legal reforms.

Suggestions

In view of India's legal and technological responses in the matter of unauthorized autonomous drone activities, these 10 suggestions are made to enhance effectiveness and fill existing regulatory and operational gaps.

1. Amend the Drone Rules to include AI-specific provisions for autonomous systems. These updates should define operational parameters, enforceability standards, and accountability mechanisms tailored to self-navigating drones.
2. Establish a dedicated regulatory body for autonomous drone oversight. This authority should centralize licensing, enforcement, and policy development specific to AI-enabled UAVs.
3. Develop a tiered penalty system based on the severity and intent of rogue drone activities. This framework should impose higher penalties for security breaches or repeated violations by autonomous systems.
4. Integrate the Digital Sky Platform with real-time AI-driven analytics. This enhancement will allow dynamic identification of unauthorized drones based on behavioral patterns and flight path anomalies.
5. Mandate AI-operational certification for drone manufacturers and developers. These certifications should cover programming accountability, safety features, and override protocols to ensure responsible development.
6. Expand the deployment of counter-drone systems to urban and border areas with high threat indices. Prioritize radar and RF sensor integration with local enforcement units to improve response speed.
7. Launch public reporting tools such as mobile applications for real-time drone sightings. These tools should be linked to central databases to verify and respond to citizen-reported threats efficiently.
8. Standardize operational protocols for the ethical use of counter-drone technologies. Protocols should include conditions for deploying destructive measures and emphasize the use of non-lethal neutralization methods in populated areas.

[26] Sagar Kulkarni, "DH Deciphers | Friendly vs rogue drone: How are they differentiated and tackled?", *Deccan Herald*, July 2, 2021.

9. Invest in domestic R&D to reduce reliance on imported counter-drone components. Encourage innovation through partnerships with defense firms like BEL to manufacture scalable, cost-effective systems.

10. Clarify liability for autonomous drone incidents through a legally codified accountability chain. Assign responsibilities across drone operators, AI developers, and hardware manufacturers to streamline redressal and deterrence.

Bibliography

- 10 Counter-Drone Technologies to Detect and Stop Drones Today, available at: https://www.robinradar.com/resources/10-counter-drone-technologies-to-detect-and-stop-drones-today (Visited on March 2, 2025).
- A Brief on Counter-Drone Technologies: Countering Rogue Drones, available at: https://www.linkedin.com/pulse/amr-future-brief-counter-drone-technologies-countering-zkmhc/ (Visited on March 1, 2025).
- Adani Defence and Aerospace at Aero India 2025, Adani Enterprises (February 2025), available at: https://www.adanienterprises.com/en/newsroom/media-releases/adani-defence-and-aerospace-and-drdo-unveil-india-s-vehicle-mounted-counter-drone-system (Visited on March 18, 2025).
- Counter-Drone Technologies: The Legal Challenges, available at: https://www.nishithdesai.com/SectionCategory/33/Technology-Law-Analysis/12/60/TechnologyLawAnalysis/4409/3.html (Visited on March 4, 2025).
- Countering Rogue Drones Menace in Absence of Real System, available at: https://bharatshakti.in/countering-rogue-drones-menace-in-absence-of-real-system/ (Visited on April 2, 2025).
- Countering Rogue Drones, available at: https://chintan.indiafoundation.in/articles/countering-rogue-drones/ (Visited on March 5, 2025).
- Countering Rogue Drones: Challenges and Technologies, available at: https://defence.capital/wp-content/uploads/2019/08/countering-rouge-drones.pdf (Visited on February 23, 2025).
- Countering Rogue Drones: Key Anti-Drone Jamming Techniques, available at: https://flymoredrone.in/blog-details/countering-rogue-drones-key-anti-drone-jamming-techniques (Visited on February 24, 2025).
- Drone Laws in India, available at: https://legalventureslawoffices.com/2024/01/31/drone-laws-in-india/ (Visited on March 11, 2025).
- Drone Threat is Real: India Needs a Comprehensive Counter-Drone Strategy, available at: https://www.vifindia.org/article/2023/june/09/Drone-Threat-is-Real-India-Needs-a-Comprehensive-Counter-Drone-Strategy (Visited on March 18, 2025).
- India's Border Security Challenge: Rogue Drones and Smuggling Surge, available at: https://borderman.in/articles/indias-border-security-challenge-rogue-drones-and-smuggling-surge/ (Visited on March 27, 2025).
- K. Bharanitharan, G. Kaur, et.al., "Drones and Surveillance Challenges and Legal Regulation Against Drone Crimes in India", 1 *ICAMAC* 104 (2024).
- My New India Story Podcast Episode 1: Countering Rogue Drones, available at: https://www.investindia.gov.in/team-india-blogs/my-new-india-story-podcast-episode-1-countering-rogue-drones (Visited on February 26, 2025).
- National Anti-Drone Guidelines, available at: https://www.drishtiias.com/daily-news-analysis/national-anti-drone-guidelines (Visited on February 27, 2025).
- National Counter Rogue Drone Guidelines, available at: https://sflc.in/policies-and-cases/national-counter-rogue-drone-guidelines/ (Visited on March 3, 2025).
- Ritika Rathi, Sreetama Sen, et.al., "Hovering over us – Drones in civil use", available at: https://corporate.cyrilamarchandblogs.com/2020/05/hovering-over-us-drones-in-civil-use/ (Visited on April 8, 2025).
- Strengthening Military Intelligence: The Role of Counter-Drone Systems, available at: https://indrajaal.in/insights/strengthening-military-intelligence-the-role-of-counter-drone-systems/ (Visited on March 14, 2025).
- What Technique Best Defeats Rogue Drones?, available at: https://www.unmannedairspace.info/commentary/what-technique-best-defeats-rogue-drones/ (Visited on February 28, 2025).